REMARKS

Claims 1-6, 8-23, and 25-37 were pending. The claims have been amended and new claims 39-41 have been added (support for claim 39 being found at page 10, lines 1-9 and page 15, line 31 through page 16, line 9; and support for new claims 40-41 at page 7, lines 1-32). The previously pending claims have been clarified to refer to malicious software, rather a virus. While the application does not use this term expressly, it is well understood by those of skill in the art to refer to the problems discussed at page 1, beginning at line 26 (e.g., worms, Trojan horses, etc.)

Claim 8 was rejected under §112, second paragraph, and has been amended as to form. Reconsideration and withdrawal of the rejection are respectfully requested.

Claims 1-6, 8-23, and 25-37 were rejected as anticipated by CHEFALAS et al. 2002/0116639. Reconsideration and withdrawal of the rejection are respectfully requested.

CHEFALAS et al. disclose a system for automatically handling viruses, where the system can be provided in a virus scanner installed on a server or client computer. The virus scanner (VSN) detects a virus and notifies the scanner controller (VSC) that the scanner has detected a virus by known virus detecting processes. The scanner disconnects the client computer from the network and disinfects the computer. The scanner notifies an administration system and may take steps to prevent

the virus from spreading to other computers (paragraphs 0025, 0028, 0050, 0051, 0054; Figures 1 and 6-7).

By contrast, the invention defined in the presently pending claims activates the malicious software in a security system for a computer. CHEFALAS et al. detect a virus, but there is no indication that the virus is activated in a security system. As will be appreciated by those of skill in the art, the security system presents a secure environment in which to activate the malicious software, in order to contain the potential damage to the security system.

Specifically, CHEFALAS et al. do not disclose a security system with a first sub-system that activates unknown malicious software and that detects the activated unknown malicious software by detecting consequences of activation of the malicious software. The reference merely discloses traditional virus detection and the ability to disconnect the infected computer. The present invention seeks to avoid infecting the computer by activating the malicious software in a security system for the computer.

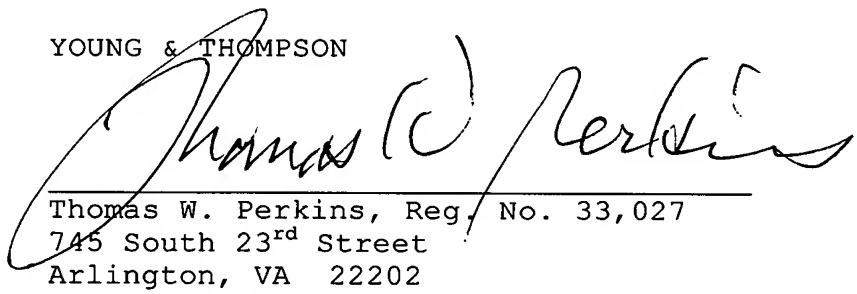
Accordingly, the claims avoid the rejection under §102 and allowance of all pending claims is respectfully requested.

In view of the present amendment and the foregoing remarks, it is believed that the present application has been placed in condition for allowance. Reconsideration and allowance are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Thomas W. Perkins, Reg. No. 33,027
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

TWP/lk